# Windows XP Professional

# Security Assessment Guide

## January 28, 2003

## DRAFT

Prepared by:
Barre Bull, Technical Director for InfoSec Services
Richard Sella, Sr. Security Engineer

Science Applications International Corporation
An Employee-Owned Company
13921 Park Center Road
Suite 300
Herndon, VA 20171

SAIC-6663-2003-032

Prepared for:
Mr. Greg Montgomery
U.S. Department of Agriculture
Room 431-W
Whitten Building
14th and Independence
Washington, D.C. 20250

**For Official Use Only**

U.S. Department of Agriculture
Washington, D.C. 20250

# USDA Microsoft Windows XP Professional Security Assessment Guide

## 1. PURPOSE

This Security Assessment Guide is designed to assist Agency ISSPMs in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in DR 3140-001, "USDA Information Systems Security Policy." By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

## 2. SCOPE

This guide is to be used by all USDA organizational elements to help assess the security posture of Microsoft Windows XP Professional. This checklist is ***not intended to be a configuration guide*** but a tool to assist in determining if the system meets the requirements for a Sensitive But Unclassified (SBU) system and assessing the vulnerabilities, both current and potential, of the system. The checks performed are based on Federal, USDA, and Best Security Practices for the protection of SBU data. This checklist does not address applications installed on the system or special purpose configurations (i.e. web servers, database servers, etc.).

## 3. BACKGROUND

Risk Assessments are mandated by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." A security risk assessment process is a comprehensive evaluation of the system's technical and non-technical security features. It establishes the extent that a specific design and implementation meets specific security requirements. USDA does not currently have a comprehensive security risk assessment process. This guide is intended to serve as an interim measure, until formal risk assessment policies and procedures can be developed and implemented.

## 4. REFERENCES

a. External

(1) Public Law 100-235, "Computer Security Act of 1987"
(2) Public Law 93-579, "Privacy Act of 1974"
(3) Public Law 93-502, "Freedom of Information Act"
(4) Public Law 99-474, "Computer Fraud and Abuse Act"
(5) OMB Circular No. A-130 Appendix III, "Security of Federal Automated Information Resources," revised February 8, 1996.
(6) OMB Circular No. A-123, "Management Accountability and Control," June 29, 1995.

b. USDA Internal Regulations

(1) DR 3140-001, "USDA Information Systems Security Policy" dated may 15, 1996
(2) DM 3140-1 "USDA Management ADP Security Manual" dated March 5, 1992

# Windows XP Professional Assessment Guide

This assessment should be completed by the Agency's ISSPM or designated alternate in conjunction with the Agency Assessment Checklist. Answer all questions. Provide supplemental information as appropriate. All "No" and "Partial" answers must include supplemental information (such as the given reason why the requirement cannot be met) and an action plan that describes how the requirement will be met or mitigated, as well as a schedule for completion of the plan. Typically, this would be done by developing the action plan in this document and reflecting this in the security plan for the agency.

**Agency/System Identification:**

| | |
|---|---|
| Agency<br>(Agency, Office, Bureau, Service, etc.): | |
| Address | |
| Date of last Assessment: | |

| | | | |
|---|---|---|---|
| Test Number: **1** | SITE/SYSTEM: | DATE: | TIME: |
| Test Name: Microsoft Windows XP Professional Workstation Access and Configuration | | | |
| Resources Required: | Access to a Microsoft Windows XP Professional Workstation, Valid Administrator and non-Administrator user account. | | |
| Personnel Required: | Microsoft Windows XP Professional Administrator. | | |
| Objectives: | To determine that the Microsoft Windows XP Professional Workstations are configured to meet USDA requirements pertaining to systems protection, user access privileges and virus protection. | | |
| Procedure Description: (Summary) | Verify that access is properly controlled; virus protection software is installed, configured and functioning properly. Verify version and service pack level of operating system. | | |

## Detailed Procedures and Results

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **1.** | Observe that the system to be assessed is logged off or that a password protected screensaver has been implemented. | System is logged off or a password-protected screensaver is active. | | |
| **2.** | If a user is logged into the system then log off the system. | User is logged off the system. | | |
| **3.** | Ask the System Administrator if the CMOS on all workstations are password protected. | The CMOS on all workstations are password protected. | | |
| **4.** | Ask the System Administrator if the workstation CMOS has been configured to boot only from the hard drive. | The workstation CMOS has been configured to boot only from the hard drive. | | |
| **5.** | Use the Secure Attention Sequence (**Ctrl+Alt+Delete**) to access the workstation logon screen. | Logon screen appears. | | |
| **6.** | Verify a Legal Notice dialog box appears prior to the Logon dialog box with an appropriate warning similar to the text used in **Attachment 1**. | A Legal Notice dialog box appears prior to the Logon dialog box similar to the text in Attachment 1. | | |

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **7.** | Click the **OK** button in the Legal Notice dialog and continue with log on. | Logon Dialog window is presented on screen. | | |
| **8.** | Verify that there is no User ID from a previous session in the User ID portion of the logon window. | There is no User ID from a previous session in the User ID portion of the logon window. | | |
| **9.** | Verify that the **XP Welcome Screen** does "NOT" appear and the **Windows 2000/XP** secure style login screen appears.<br>**(See Attachment 2A and 2B)** | XP Welcome screen does not appear.<br>**NOTE:** The XP Welcome screen lists user names that an end user can select from when they log into the system. This is an unnecessary security risk. | | |
| **10.** | Observe how many buttons are available on the logon window. | 4 radio buttons are available on the logon window, the OK, Cancel, Shutdown…, and Options button. The Shutdown button is grayed out. | | |
| **11.** | Ask the SA if the **Guest** account has a password. | Guest account has a password. | | |
| **12.** | Attempt to logon to the system using the User ID **Guest** and pressing return (do not enter a password). | Access denied. | | |
| **13.** | Attempt to logon to the system using the User ID **Guest** and enter **Guest** for the password. | Access denied. | | |
| **14.** | Attempt to logon to the system using the User ID **Administrator** and pressing return (do not enter a password). | Access denied. | | |
| **15.** | Attempt to (or have system administrator) logon to the system using a valid non-administrator User ID and password. | Logon is completed | | |
| **16.** | Ask the System Administrator if **local** or **centralized** virus scanning is used. | If centralized virus scanning is used skip to question 19. | | |

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **17.** | When the desktop appears observe the system tray in the bottom right corner of the desktop to verify that a virus protection software icon is present. | Virus protection software icon is present. | | |
| **18.** | Have SA show the date of the virus patterns/signatures currently running. | The patterns/signatures should be no more than one month old, go to step 21. | | |
| **19.** | If centralized virus scanning is used ask the System Administrator if the virus signatures are kept current on the central scanning system. | Most current version of the virus signatures are being used. | | |
| **20.** | Have SA show the date of the virus patterns/signatures currently running. | The patterns/signatures should be no more than one month old. | | |
| **21.** | Right-click on the desk top and select **Properties**. | Display Properties window opens. | | |
| **22.** | Select the **Screen Saver** tab. | ♦ A screensaver has been selected.<br>♦ The **On resume, password protect** box is checked.<br>♦ The **Wait time** is set to a maximum of 15 minutes. | | |
| **23.** | Close **Display Properties** window. | Display Properties window closes. | | |
| **24.** | Click **Start** menu, select **All Programs** and observe the programs listed. | Only USDA approved programs are listed in the menu. | | |
| **25.** | Ask the SA if shared files are protected from unauthorized access and modification using rights and permissions assignment. | Shared files are protected from unauthorized access and modification using rights and permissions assignment. | | |
| **26.** | Click on the **Start** button in the Task Bar. | Start menu choices appear. | | |
| **27.** | Click on **Control Panel** icon. | Control Panel window opens. | | |
| **28.** | Close **Control Panel** window. | Control Panel window closes. | | |
| **29.** | Click on the **Start** button in the Task Bar. | Start menu choices appear. | | |
| **30.** | Right click on the **My Computer** Icon and select **Properties**. | System Properties dialog box opens. | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **31.** | Select the **General** tab and verify that the Operating System is **Microsoft Windows XP Professional**. | The operating system is Microsoft Windows XP Professional. | | |
| **32.** | Verify that the current Service Pack is installed. | The current Service Pack has been installed. | | |
| **33.** | Ask the SA if all recommended and critical updates have been installed from the Microsoft Windows Update web site. | All recommended and critical updates have been installed. | | |
| **34.** | Close the **System Properties** window. | System Properties window closes. | | |
| **35.** | Log off the workstation and log back on using the workstation **Administrator** user ID and password. | Logon is completed. | | |
| **36.** | Click on the **Start** button in the Task Bar. | Start menu choices appear. | | |
| **37.** | Click on the **Control Panel** icon. | Control Panel appears. | | |
| **38.** | Click on the **Performance and Maintenance** icon. | Performance and Maintenance window opens. | | |
| **39.** | Click on the **Administrative Tools** icon. | Administrative Tools window opens. | | |
| **40.** | Click on the **Computer Management** icon. | Computer Management window opens. | | |
| **41.** | Click on the **Local Users and Groups** folder in the left window pane. | Local Users and Groups folders appear in right window pane. | | |
| **42.** | Click on the **Users** folder in either pane. | Local Users listing opens. | | |
| **43.** | Ask SA if **domain** or **local** user accounts are used to access workstations. | Test #2 will deal with the configuration of local user accounts. | | |
| **44.** | Observe that the **Administrator** account has been renamed. | Administrator account has been renamed. | | |
| **45.** | Ask the SA if the **Administrator** account is used. | Administrator account is not used. | | |
| **46.** | Observe how many user accounts are listed in the right window pane. | If Domain accounts are in use there should only be two local user accounts listed: the renamed **Administrator** account and the disabled **Guest** account. | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **47.** | Ask the SA if users requiring administrative access to workstations have individual accounts with membership in the **Administrators** Group. | Users requiring administrative access to workstations have individual accounts with membership in the Administrators Group. | | |
| **48.** | Right-click on the **Guest** icon and click **Properties**. | Guest Properties window Opens. | | |
| **49.** | Click on the **General** tab and observe that the **User cannot change password**, **Password never expires** and **Account is disabled** boxes are checked. | User Cannot Change Password, Password Never Expires and Account is Disabled boxes are checked. | | |
| **50.** | Click on the **Member Of** tab in the Guest Properties window and observe what Group(s) the **Guest** account is a member of. | Guest account is a member of Guests Group only. | | |
| **51.** | Click the **OK** button and close the **Guest Properties** dialog box window. | Guest Properties dialog window closes. | | |
| **52.** | Click on the **Local Users and Groups \| Groups** folder in the left window pane. | Groups listing opens in right window pane. | | |
| **53.** | Observe the **Groups** listing in the right window pane to ensure that only approved Groups exist. | Only Approved Groups exist. | | |
| **54.** | Observe the **Groups** listing in the right window pane to ensure that only approved Groups exist. | Only Approved Groups exist. | | |
| **55.** | Ask SA if local system rights/ permissions are assigned based on local Group memberships. | Rights/permissions are assigned based on local Group membership not individual users. | | |
| **56.** | Ask SA if server/network – rights and permissions are assigned based on domain-level group memberships. | Rights/permissions are assigned based on domain-level group's not individual users. | | |
| **57.** | Ask SA if unnecessary services have been disabled. (Click on the **Services and Applications** folder in the left window pane of the open **Computer Management** window then select **Services** to observe what services are currently running.) | Unnecessary services have been disabled. (Unnecessary services will be different from system to system in some cases and generally be determined locally.) | | |
| **58.** | Ask the SA if physical access to workstations is restricted. | Physical access is restricted. | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **59.** | Ask the SA if any wireless connections are being used to connect to the network. | No wireless connections are present on the network. | | |
| **60.** | Close the **Computer Management** window. | Computer Management Window closes. | | |
| **61.** | Close the **Administrative Tools** window. | Administrative Tools Window closes. | | |
| **62.** | Close the **Performance and Maintenance** window if open. | Performance and Maintenance window closes. | | |
| **63.** | Close the **Control Panel** window if open. | Control Panel window closes. | | |

**Comments:**

**Action Plan:**

| Test Number: **2** | SITE/SYSTEM: | DATE: | TIME: |
|---|---|---|---|
| Test Name: Microsoft Windows XP Professional Workstation Password Policy Configuration (This test is required only if users are allowed to have local access to the workstation accounts.) | | | |
| Resources Required: | Access to a Microsoft Windows XP Professional Workstation with Administrator Access. | | |
| Personnel Required: | Microsoft Windows XP Professional Workstation Administrator. | | |
| Objectives: | To determine that the Microsoft Windows XP Professional Workstation Password Policies are configured to meet USDA requirements pertaining to Identification and Authentication. | | |
| Procedure Description: (Summary) | Verify that Password Policies are properly configured. | | |

## Detailed Procedures and Results

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **1.** | Click on the **Start** button in the Task Bar. | Start menu choices appear. | | |
| **2.** | Select **Control Panel**. | Control Panel window appears. | | |
| **3.** | Click on the **Performance and Maintenance** icon. | Performance and Maintenance window opens. | | |
| **4.** | Click on the **Administrative Tools** icon. | Administrative Tools window opens. | | |
| **5.** | Click on the **Local Security Policy** icon. | Local Security Settings window opens. | | |
| **6.** | Click on the **Account Policies** folder in the left window pane of the Local Security Policy window. | Password Policy and Account Lockout Policy folders appear in the right window pane. | | |
| **7.** | Verify that the **Password Policy** and **Account Lockout Policy** match those pictured on the Workstation Account Policy settings attachments.<br>**(See Attachment 3A and 3B)** | The account policies match those on the workstation Account Policy Settings attachments, go to Step 19. If not, continue with Step 8. | | |
| **8.** | Click on the **Password Policy** folder in the left window pane. | Password Policy settings open in right window pane. | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| 9. | Set **Enforce password history** to 5 passwords remembered by right-clicking policy and selecting **Properties**. | Security Setting = 5 passwords remembered. | | |
| 10. | Set **Maximum password age** to 90 days by right-clicking policy and selecting **Properties**. | Security Setting = 90 days. | | |
| 11. | Set **Minimum password age** to 7 days by right-clicking policy and selecting **Properties**. | Security Setting = 7 days. | | |
| 12. | Set **Minimum password length** to 8 characters by right-clicking policy and selecting **Properties**. | Security Setting = 8 characters. | | |
| 13. | Set **Passwords must meet complexity requirements** to Enabled by right-clicking policy and selecting **Properties**. | Security Setting = Enabled. | | |
| 14. | Set **Store password using reversible encryption for all users in the domain** to Enabled by right-clicking policy and selecting **Properties**. | Security Setting = Enabled. | | |
| 15. | Click on the **Account Lockout Policy** in the left window pane. | Account Lockout policies appear in right window pane. | | |
| 16. | Set **Account lockout duration** to 0 to enable by right-clicking policy and selecting **Properties.** Lockout Forever – Until unlocked by Administrator. | Security Setting = 0. | | |
| 17. | Set **Account lockout threshold** to 3 in-valid login attempts by right-clicking policy and selecting **Properties**. | Security Setting = 3 in-valid login attempts. | | |
| 18. | Set **Reset account lockout counter after** to 60 minutes by right-clicking policy and selecting **properties**. This setting has no real affect if **Account lockout duration** is set to 0. | Security Setting = 60 minutes. | | |
| 19. | Close the **Local Security Settings** window. | Local Security Settings window closes. | | |
| 20. | Close the **Administrative Tools** Window. | Administrative Tools window closes. | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **21.** | Close the **Performance and Maintenance** window if open. | Performance and Maintenance window closes. | | |
| **22.** | Close the **Control Panel** Window if open. | Control Panel window closes. | | |

| |
|---|
| **COMMENTS:** |
| **ACTION PLAN:** |

| Test Number: **3** | SITE/SYSTEM: | DATE: | TIME: |
|---|---|---|---|
| Test Name: Microsoft Windows XP Professional Workstation General Registry Settings | | | |
| Resources Required: | Administrative access to a Microsoft Windows XP Professional Workstation. | | |
| Personnel Required: | Microsoft Windows XP Professional Workstation Administrator. | | |
| Objectives: | To verify that general registry settings are in place and are correctly configured. | | |
| Procedure Description: (Summary) | Using Regedt32 to access the system registry and verify that specific registry keys are correctly configured. **WARNING: This test must be done carefully to prevent any damage to the registry. DO NOT attempt to edit the registry!** | | |

## Detailed Procedures and Results

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **1.** | Click on the **Start** button in the Task Bar. | Start menu choices appear. | | |
| **2.** | Click on the **Run** icon. | Run Dialog window opens. | | |
| **3.** | Enter **Regedt32** in the Run dialog box and click **OK**. | Regedt32 starts and the Registry tree appears in the left window. | | |
| **4.** | Double-Click on the **HKEY_LOCAL_MACHINE** folder in the left window pane. | HKEY_LOCAL_MACHINE categories appear in right window pane. | | |
| **5.** | Right-Click on the **HKEY_LOCAL_MACHINE** folder in the left window pane and select **Permissions**. | Registry Permissions dialog window opens. | | |
| **6.** | Ensure Permissions are correct. | Permissions on "HKEY_LOCAL_MACHINE" are set to:<br>**Administrators-**Full Control<br>**Everyone**-Read Only<br>**System**-Full Control | | |
| **7.** | Select the **Advanced** button in the **Permissions for HKEY_LOCAL_MACHINE** dialog box and select the **Permissions tab.** Ensure that the check box for **Replace permission entries on all child objects with entries shown here that apply to child objects** is "NOT CHECKED". | The check box for Replace permission entries on all child objects with entries shown here that apply to child objects is "NOT CHECKED". | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| 8. | Select the **Auditing Tab** and ensure that the **Inherit from parent the auditing entries that apply to child objects. Include these with entries explicitly defined here** is not checked. | Inherit from parent the auditing entries that apply to child objects. Include these with entries explicitly defined here checkbox is not selected. | | |
| 9. | Select the **Everyone** group from the **Auditing Entries:** window to ensure that all **Successful** and **Failed** checkboxes are selected. | All Successful and Failed checkboxes are selected. | | |
| 10. | Close the **Auditing Entry**, **Advanced Security Settings** and **Permissions** dialog box windows. | Auditing Entry, Advanced Security Settings and Permissions dialog windows close. | | |
| 11. | Select the **HKEY_LOCAL_MACHINE\ Software\Program Groups** folder in the left window pane. Next, right-Click and select **Permissions**. | Registry Permissions dialog window opens. | | |
| 12. | Select the **Advanced** button in the **Permissions for Program Groups** dialog box and select the **Auditing tab**. Select the **Everyone** group from the **Auditing Entries:** window to ensure that all **Successful** and **Failed** checkboxes are selected. | All Successful and Failed check boxes are selected. | | |
| 13. | Click **OK** in the **Auditing Entry for Program Groups** window. | Changes are successfully saved and window closes. | | |
| 14. | Click **OK** in the **Advanced Security Settings for Program Groups** window. | Advanced Security Settings for Program Groups window closes. | | |
| 15. | Click **OK** in the **Permissions for Program Groups** window. | Permissions for Program Group window closes. | | |
| 16. | Double-Click on the **Software/Microsoft** folder in the left window pane. | Microsoft categories appear in right window pane. | | |
| 17. | Double-Click on the **Software/Microsoft/Windows NT** folder in the left window pane. | Windows NT categories appear in right window pane. | | |
| 18. | Double-Click on the **Windows NT/Current Version** folder in the left window pane. | Current Version categories appear in right window pane. | | |

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **19.** | Double-Click on the **Current Version\ Winlogon** folder in the left window pane. | Winlogon categories appear in right window pane. | | |
| **20.** | Observe the **AltDefaultUserName** entry in the right window pane and verify that a "1" appears in the String Editor. | A "1" appears in the String Editor. | | |
| **21.** | Observe the **LegalNoticeCaption** in the right window pane and verify that the text string is "AUTHORIZED USE ONLY." | The text string within the double quotes is "AUTHORIZED USE ONLY." | | |
| **22.** | Observe the **LegalNoticeText** in the right window pane and verify that it is equivalent to the text in Attachment 1. | The text within the double quotes is equivalent to the text in the Attachment 1. | | |
| **23.** | Observe the **ShutdownWithoutLogon** entry in the right window pane and verify that a "0" appears in the String Editor. | ShutdownWithoutLogon value is set to 0. | | |
| **24.** | Close all of the **Software** hive categories in the left window pane. | All Software hive categories are closed. | | |
| **25.** | Double-Click on the **HKEY_LOCAL_MACHINE\SYSTEM** folder in the left window pane. | Hive categories appear. | | |
| **26.** | Observe the **Optional** entry in the right window pane and verify that there are no values listed or the listing does not exist. | Optional entry does not exist or No values are listed. | | |
| **27.** | Double-Click on the **SYSTEM\CurrentControlSet** folder in the left window pane. | CurrentControlSet categories appear in right window pane. | | |
| **28.** | Double-Click on the **CurrentControlSet\Control** folder in the left window pane. | Control categories appear in right window pane. | | |
| **29.** | Double-Click on the **Control\LSA** folder in the left window pane. | LSA categories appear in right window pane. | | |
| **30.** | Observe the **restrictanonymous** entry is present in the right window pane and the value is set to 1. | RestrictAnonymous value is present and set to 1.<br>**Note**: This setting restricts anonymous users from being able to obtain public information about the LSA component of the | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| | | Windows NT Security Subsystem. The LSA handles aspects of security administration on the local computer, including access and permissions. | | |
| **31.** | Double-Click on the **Control\Session Manager** folder in the left window pane. | Session Manager categories appear in right window pane. | | |
| **32.** | Observe the **ProtectionMode** entry is present in the right window pane and the value is set to 1. | ProtectionMode value is present and set to 1.<br>**Note:** This setting is necessary to further heighten security of the base objects. Among other things, it prevents users from gaining local administrator privileges by way of a dynamic-link library (DLL). | | |
| **33.** | Double-Click on the **Session Manager\SubSystems** folder in the left window pane. | SubSystems categories appear in right window pane. | | |
| **34.** | Observe that the **Posix** and **OS/2** entries are not present in the right window pane. | There are no entries for Posix and OS/2.<br>**Note:** C2-like compliance cannot be achieved unless Posix and OS/2 are removed. | | |
| **35.** | Close all **HKEY_LOCAL_MACHINE** folders. | All HKEY_LOCAL_MACHINE folders are closed. | | |
| **36.** | Right-Click on the **HKEY_CLASSES_ROOT** folder in the left window pane and select **Permissions**. | Registry Permissions dialog window opens. | | |
| **37.** | Ensure Permissions are correct. | Permissions on “HKEY_CLASSES_ROOT” and all its subkeys are set to:<br>**Administrators** - Full Control<br>**CREATOR OWNER** - Full Control<br>**Everyone** - Read<br>**System** - Full Control | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **38.** | Select the **Advanced** button then select the **Permissions tab.** Ensure that the check box for **Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here** is “NOT” selected. | Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here is not selected.<br>**NOTE:** If check box is grayed out, then step passes test. | | |
| **39.** | Close the **Advanced Security Settings** and **Permissions** dialog windows. | Advanced and Permissions dialog windows close. | | |
| **40.** | Close all **HKEY_CLASSES_ROOT** folders. | All HKEY_CLASSES_ROOT folders close. | | |
| **41.** | Double-Click on the **HKEY_USERS** folder in the left window pane. | HKEY_USERS categories appear in right window pane. | | |
| **42.** | Double-Click on the **HKEY_USERS\.DEFAULT** folder in the left window pane. | HKEY_USERS\.DEFAULT categories appear in right window pane. | | |
| **43.** | Right-Click on the **\.DEFAULT \UNICODE Program Groups** folder in the left window pane and select **Permissions**. | Permissions on "HKEY_USERS\.DEFAULT \UNICODE Program Groups\[all subkeys]" are set to:<br>**Administrators** - Full Control<br>**Everyone** - Read<br>**System** - Full Control | | |
| **44.** | Close the **Permissions for UNICODE Program Groups** dialog window. | Permissions dialog window closes. | | |
| **45.** | Close the **Registry Editor** Window. | Registry Editor Window closes. | | |

**Comment:**

**Action Plan:**

| | | | |
|---|---|---|---|
| Test Number: **4** | SITE/SYSTEM: | DATE: | TIME: |
| Test Name: Microsoft Windows XP Professional Workstation Audit | | | |
| Resources Required: | Access to a Microsoft Windows XP Professional Workstation with Administrator Access. | | |
| Personnel Required: | Microsoft Windows XP Professional Workstation Systems Administrator. | | |
| Objectives: | To determine that the Microsoft Windows XP Professional Workstations are configured to meet USDA requirements pertaining to Auditing. | | |
| Procedure Description: (Summary) | Verify that auditing is turned on, functioning and properly configured. Also, verify that the audit logs are reviewed on a regular basis and backed up on a regular schedule. | | |

## Detailed Procedures and Results

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **1.** | Ask the SA if there is a documented schedule for the review of the Audit logs. | Audit logs are reviewed per documented schedule or at least once per week. | | |
| **2.** | Ask the SA if the audit logs are backed up according to a routine schedule. Observe back-ups of audit logs. | Audit logs are backed up according to a routine schedule. | | |
| **3.** | Ask the SA if there are procedures in place for moving the audit logs off the system when they become full. | There are procedures in place for moving the audit logs off the system when they become full. | | |
| **4.** | Ask the SA if copies of the audit log backups are stored off site. | Copies of the audit log backups are stored off site. | | |
| **5.** | Click on the **Start** button in the Task Bar. | Start menu choices appear. | | |
| **6.** | Click on the **Control Panel** icon. | Control Panel appears. | | |
| **7.** | Click on the **Performance and Maintenance** icon. | Performance and Maintenance window opens. | | |
| **8.** | Click on the **Administrative Tools** icon. | Administrative Tools window opens. | | |
| **9.** | Click on the **Computer Management** icon. | Computer Management window opens. | | |
| **10.** | Double-Click on the **Event Viewer** folder in the left window pane. | Application, Security, and System Logs appear in right window pane. | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **11.** | Right-Click on the **Application** Log and select **Properties** from the Actions menu. | Application Properties dialogue box appears. | | |
| **12.** | Select the **General** tab and verify that the **Do not overwrite events** box is checked. | "Do Not Overwrite" box is checked. | | |
| **13.** | Click the **OK** button at the bottom of the **Application Properties** dialog window. | Application Properties Settings Dialogue window closes. | | |
| **14.** | Right-Click on the **Security** Log and select **Properties** from the Actions menu. | Security Properties dialogue box appears. | | |
| **15.** | Select the **General** tab and verify that the **Do not overwrite events** box is checked. | "Do Not Overwrite" box is checked. | | |
| **16.** | Select the **Filter** tab and verify all **Event types** are checked.<br>**(See Attachment 4)** | All 5 **Event types** are checked. | | |
| **17.** | Click the **OK** button at the bottom of the **Security Properties** dialog window. | Security Properties Settings Dialogue window closes. | | |
| **18.** | Right-Click on the **System** Log and select **Properties** from the Actions menu. | System Properties dialogue box appears. | | |
| **19.** | Select the **General** tab and verify that the **Do not overwrite events** box is checked. | "Do Not Overwrite" box is checked. | | |
| **20.** | Click the **OK** button at the bottom of the **System Properties** dialog window. | System Properties dialogue window closes. | | |
| **21.** | Close the **Computer Management** window. | Computer Management Window closes. | | |
| **22.** | Close the **Administrative Tools** Window. | Administrative Tools window closes. | | |
| **23.** | Close the **Performance and Maintenance** window if open. | Performance and Maintenance window closes. | | |
| **24.** | Close the **Control Panel** Window if open. | Control Panel window closes. | | |

**Comments:**

**Action Plan:**

| Test Number: **5** | SITE/SYSTEM: | DATE: | TIME: |
|---|---|---|---|
| Test Name: Microsoft Windows XP Professional Workstation System Backups | | | |
| Resources Required: | Access to a Microsoft Windows XP Professional Workstation with Administrator Access. | | |
| Personnel Required: | Microsoft Windows XP Professional Workstation Administrator. | | |
| Objectives: | To ensure that Microsoft Windows XP Professional Workstations operating systems, applications and data are backed up on a timely basis and that the backup procedures are being performed. | | |
| Procedure Description:<br>(Summary) | Examine backup scheduler program and log files to determine that backups are conducted on a timely basis. Review Windows XP Professional Workstation backup procedures and determine that procedures are being performed. | | |

## Detailed Procedures and Results

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **1.** | Log onto workstation as Administrator. | Successful log-on. | | |
| **2.** | Review backup scheduler programs and log files to determine that backups are conducted on a timely basis. | Backups are conducted on a timely basis. | | |
| **3.** | Ask Administrator for the documented workstation backup procedures and ask if the procedures are being followed. | Documented workstation backup procedures are available and are being followed as required. | | |
| **4.** | Ask SA if copies of the backups are regularly stored in a secure off-site location. | Copies of backups are regularly stored in a secure off-site location. | | |

| |
|---|
| **Comments:** |
| **Action Plan:** |

| | | | |
|---|---|---|---|
| Test Number: **6** | SITE/SYSTEM: | DATE: | TIME: |
| Test Name: Microsoft Windows XP Professional Workstation Local Security Policy Settings (This test is required only if Local Security Policies are used instead of Domain-level Security Policies.) | | | |
| Resources Required: | Access to a Microsoft Windows XP Professional Workstation with Administrator Access | | |
| Personnel Required: | Microsoft Windows XP Professional Workstation Administrator. | | |
| Objectives: | To ensure that Microsoft Windows XP Professional Workstations are configured to meet USDA requirements pertaining to Local Security policies. | | |
| Procedure Description: (Summary) | Examine Local Security Policy settings to determine workstation security settings are set to the correct values. Review Windows XP Professional Workstation Local Policy settings and determine that the correct settings are implemented. **NOTE: Any Domain-level Security policy will override any Local Security policy.** | | |

## Detailed Procedures and Results

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **1.** | Click on the **Start** button in the Task Bar. | Start menu choices appear. | | |
| **2.** | Click on the **Control Panel** icon. | Control Panel appears. | | |
| **3.** | Click on the **Performance and Maintenance** icon. | Performance and Maintenance window opens. | | |
| **4.** | Click on the **Administrative Tools** icon. | Administrative Tools window opens. | | |
| **5.** | Click on the **Local Security Policy** icon. | Local Security Settings window opens. | | |
| **6.** | Double-Click on the **Local Policies** folder in the left window pane. | Local Policies appear in right window pane. | | |
| **7.** | Double-Click on the **Local Policies/Security Options** folder in the left window pane.<br>**(See Attachment 5)** | Security Options appear in right window pane. | | |
| **8.** | Verify the **Devices: Restrict CD-ROM access to locally logged-on user only** is set to **Enabled** in the right window pane. | Restrict CD-ROM access to locally logged-on user only is enabled. | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **9.** | Verify the **Devices: Restrict floppy access to locally logged-on user only** is set to **Enabled** in the right window pane. | Restrict floppy access to locally logged-on user only is enabled. | | |
| **10.** | Verify the **Interactive logon: Do not display last user name** is set to **Enabled** in the right window pane. | Do not display last user name is enabled. | | |
| **11.** | Close the **Local Security Settings** window. | Local Security Settings Window closes. | | |
| **12.** | Close the **Administrative Tools** Window. | Administrative Tools window closes. | | |
| **13.** | Close the **Performance and Maintenance** window if open. | Performance and Maintenance window closes. | | |
| **14.** | Close the **Control Panel** Window if open. | Control Panel window closes. | | |

**Comments:**

**Action Plan:**

| Test Number: **7** | SITE/SYSTEM: | DATE: | TIME: |
|---|---|---|---|
| Test Name: Microsoft Windows XP Professional Workstation Internet Connection Firewall Settings | | | |
| Resources Required: | Access to a Microsoft Windows XP Professional Workstation with Administrator Access. | | |
| Personnel Required: | Microsoft Windows XP Professional Workstation Administrator. | | |
| Objectives: | To ensure that Microsoft Windows XP Professional Workstations Internet Connection Firewall (ICF) settings are correct. | | |
| Procedure Description: (Summary) | Examine Internet Connection Firewall settings to determine that workstation settings are set to the correct values. Review Windows XP Professional Workstation Internet Connection Firewall settings and determine that the correct settings are implemented. | | |

## Detailed Procedures and Results

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **1.** | Click on the **Start** button in the Task Bar. | Start menu choices appear. | | |
| **2.** | Click on the **Control Panel** icon. | Control Panel appears. | | |
| **3.** | Click on the **Network and Internet Connections** icon. | Network and Internet Connections window opens. | | |
| **4.** | Click on the **Network Connections** icon. | Network Connections window opens. | | |
| **5.** | Right-Click on the **Local Area Connections** icon and select **Properties**. | Local Area Connections Properties window opens. | | |
| **6.** | Click on the **Advanced** tab. | Internet Connection Firewall properties are displayed. | | |
| **7.** | Ensure that the **Protect my computer and network by limiting or preventing access to this computer from the Internet** check box is “NOT” selected.<br>**(See Attachment 6)** | Check box is “NOT” selected.<br>**NOTE:** ICF should not be enabled because it may conflict with network management, scanning, or other security software. This is a good setting for stand-alone systems, not enterprise systems. | | |

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **8.** | Close the **Local Area Connections Properties** dialog window. | Local Area Connections Properties dialog window closes. | | |
| **9.** | **NOTE:** Steps 5 through 8 must be completed on all **Local Area Connection X** icons (Interfaces/NICs) listed in the **Network Connections** window. | Repeat steps 5 through 8 for each Local Area Connection icons (network interface/ NIC) listed in the Network Connections window. | | |
| **10.** | Close the **Network Connections** window. | Network Connections window closes. | | |
| **11.** | Close the **Network and Internet Connections** window if open. | Network and Internet Connections window closes. | | |
| **12.** | Close the **Control Panel** Window if open. | Control Panel window closes. | | |

**Comments:**

**Action Plan:**

| Test Number: **8** | SITE/SYSTEM: | DATE: | TIME: |
|---|---|---|---|
| Test Name: Microsoft Windows XP Professional Workstation Partition Settings | | | |
| Resources Required: | Access to a Microsoft Windows XP Professional Workstation with Administrator Access. | | |
| Personnel Required: | Microsoft Windows XP Professional Workstation Administrator. | | |
| Objectives: | To ensure that Microsoft Windows XP Professional Workstations Partition Settings are correct. | | |
| Procedure Description: (Summary) | Examine Partition Settings to determine that workstation settings are set to the correct values. Review Windows XP Professional Workstation Partition Settings and determine that New Technology File System (NTFS) partitions are implemented on all hard drive partitions. | | |

## Detailed Procedures and Results

| Step # | Procedure Description | Expected Results | Actual Results (If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **1.** | Click on the **Start** button in the Task Bar. | Start menu choices appear. | | |
| **2.** | Click on the **Control Panel** icon. | Control Panel appears. | | |
| **3.** | Click on the **Performance and Maintenance** icon. | Performance and Maintenance window opens. | | |
| **4.** | Click on the **Administrative Tools** icon. | Administrative Tools window opens. | | |
| **5.** | Click on the **Computer Management** icon. | Computer Management window opens. | | |
| **6.** | Double-Click on the **Disk Management** folder in the left window pane. | Partition settings appear in right window pane. | | |
| **7.** | Verify all hard disk partitions are formatted with **NTFS** partitions and no **FAT** partitions exist.<br>**(See Attachment 7)** | All hard disk partitions are formatted with NTFS partitions and no FAT partitions exist.<br>**NOTE:** NTFS partitions provide more security than any other partition scheme. | | |
| **8.** | Close the **Computer Management** window. | Computer Management window closes. | | |
| **9.** | Close the **Administrative Tools** Window. | Administrative Tools window closes. | | |
| **10.** | Close the **Performance and Maintenance** window if open. | Performance and Maintenance window closes. | | |

| Step # | Procedure Description | Expected Results | Actual Results<br>(If different from Expected) | Y/N/P |
|---|---|---|---|---|
| **11.** | Close the **Control Panel** Window if open. | Control Panel window closes. | | |

| |
|---|
| **Comments:** |
| **Action Plan:** |

## ATTACHMENT 1

### Legal Notice Text string:

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT…

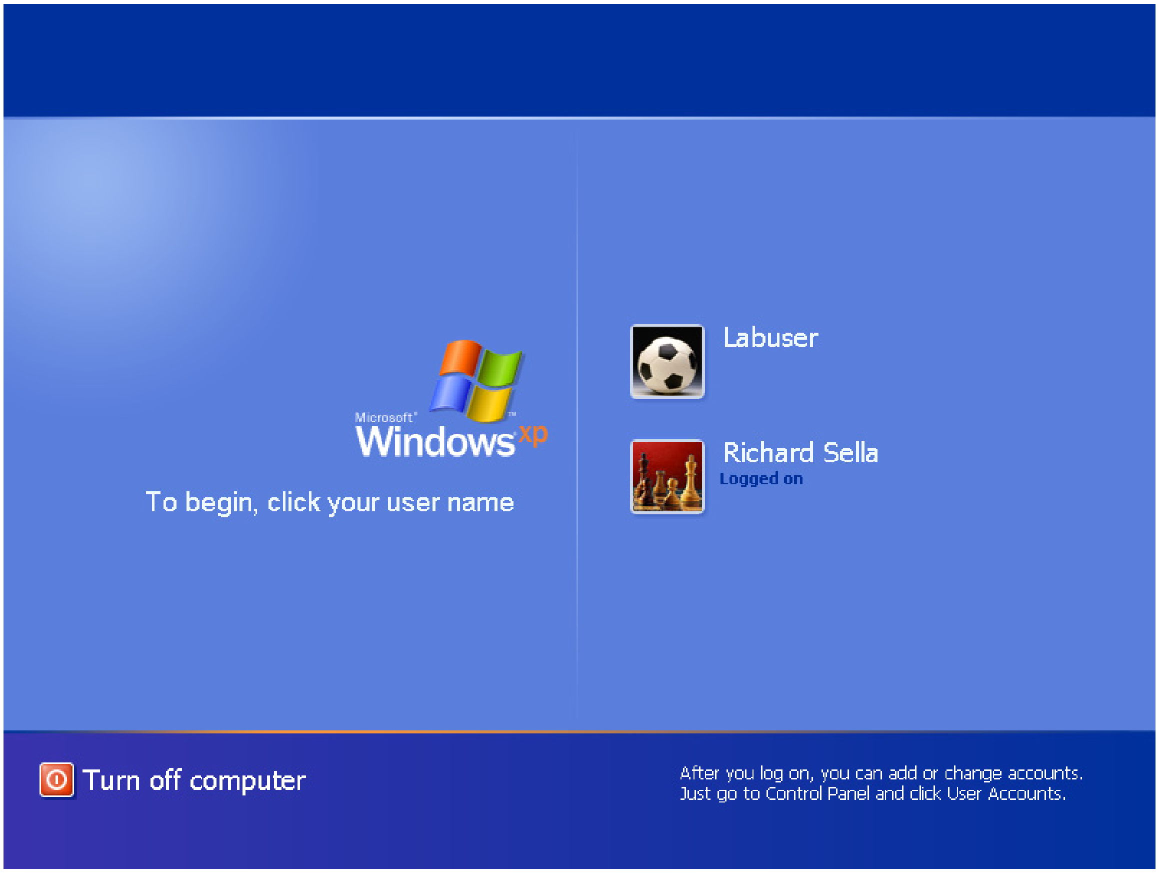
***Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.***

All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials.

**REPORT UNAUTHORIZED USE TO AN INFORMATION SYSTEMS SECURITY OFFICER**

## ATTACHMENT 2A

Microsoft Windows XP Professional Workstation Incorrect Login Screen:

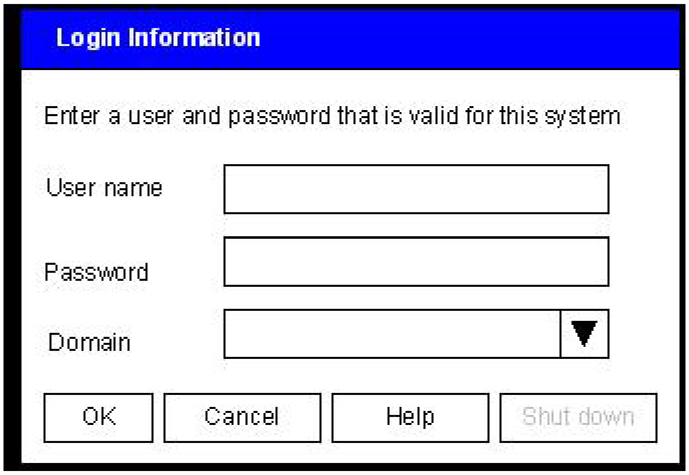


To begin, click your user name

After you log on, you can add or change accounts.
Just go to Control Panel and click User Accounts.

## ATTACHMENT 2B

Microsoft Windows XP Professional Workstation Correct Login Screen (approximation):

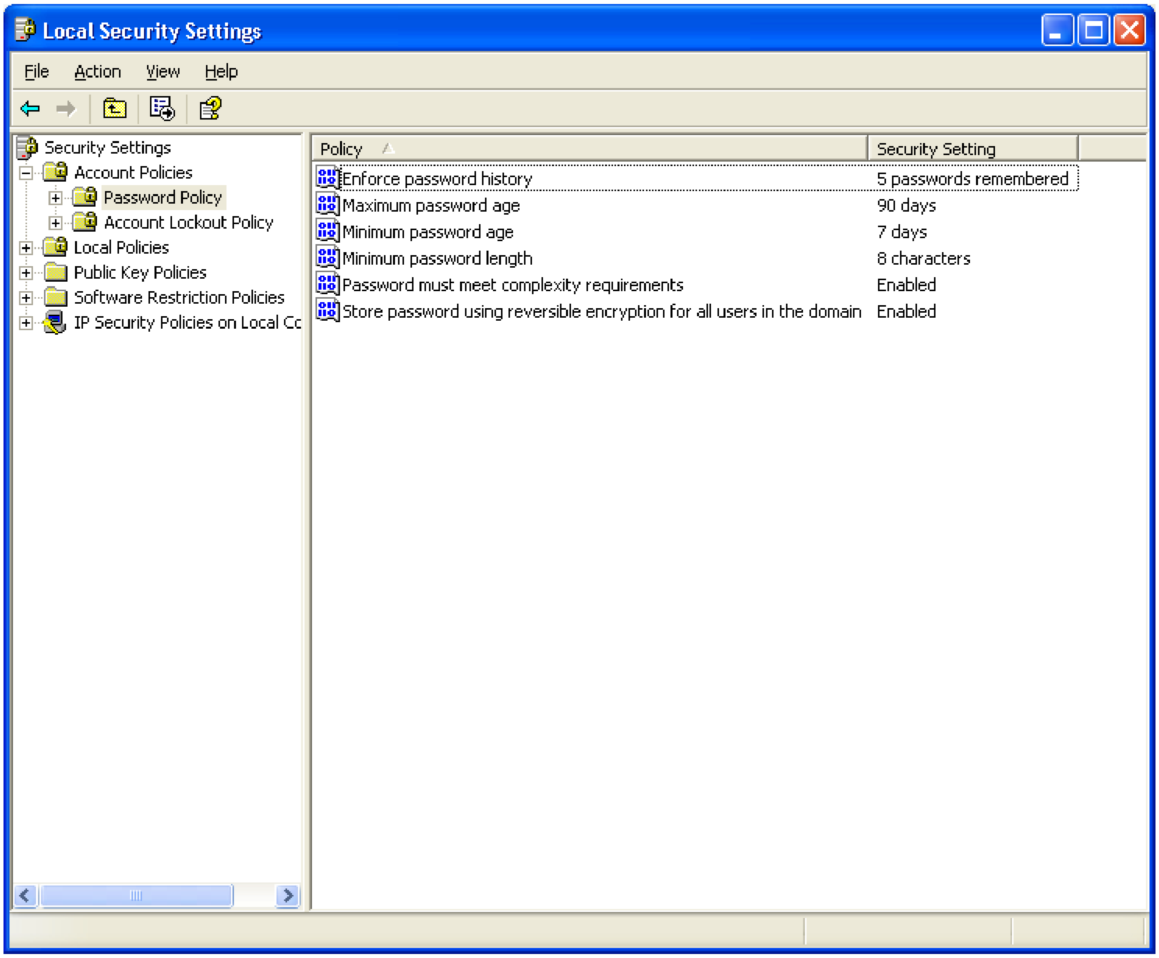


Login Information

Enter a user and password that is valid for this system

## ATTACHMENT 3 A

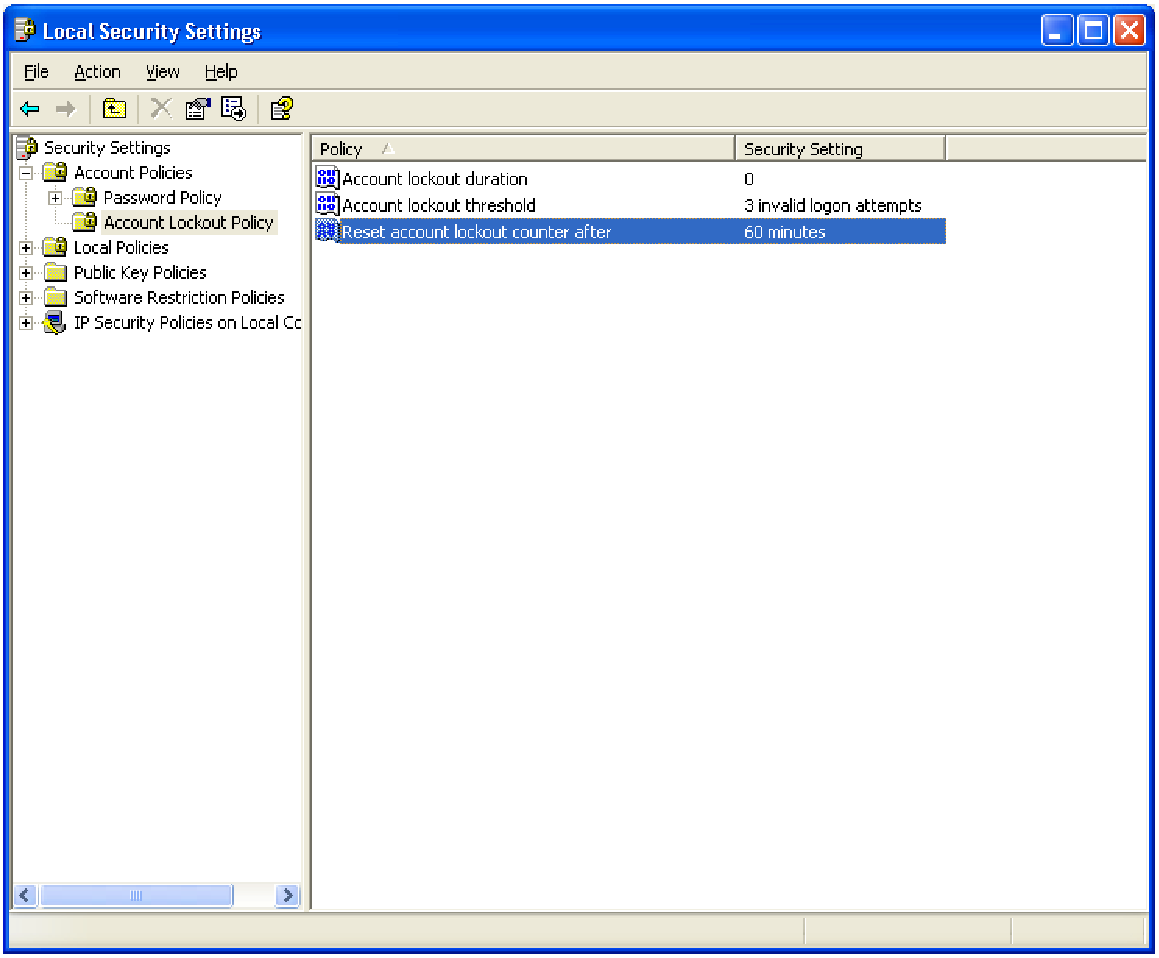
Microsoft Windows XP Professional Workstation Password Policy Settings:



| Policy | Security Setting |
|---|---|
| Enforce password history | 5 passwords remembered |
| Maximum password age | 90 days |
| Minimum password age | 7 days |
| Minimum password length | 8 characters |
| Password must meet complexity requirements | Enabled |
| Store password using reversible encryption for all users in the domain | Enabled |

## ATTACHMENT 3 B

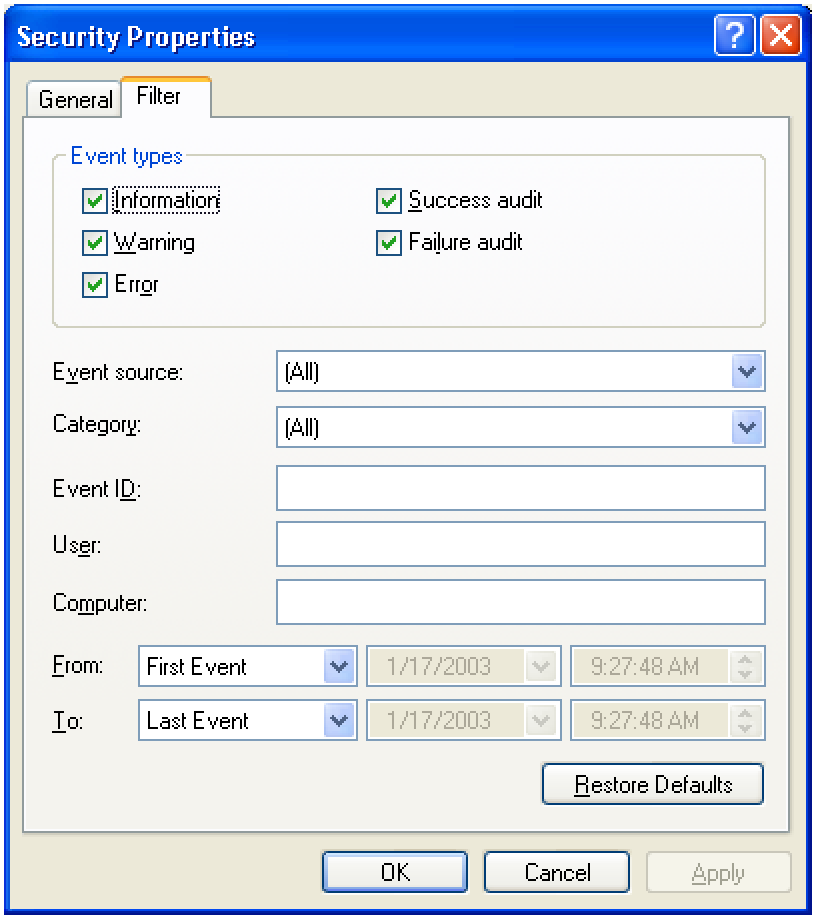
Microsoft Windows XP Professional Workstation Account Lockout Policy Settings:



| Policy | Security Setting |
|---|---|
| Account lockout duration | 0 |
| Account lockout threshold | 3 invalid logon attempts |
| Reset account lockout counter after | 60 minutes |

## ATTACHMENT 4

Microsoft Windows XP Professional Workstation Security Log Properties:



Security Properties

Event types

☑ Information

☑ Warning

☑ Error

☑ Success audit

☑ Failure audit

Event source: (All)

Category: (All)

Event ID:

User:

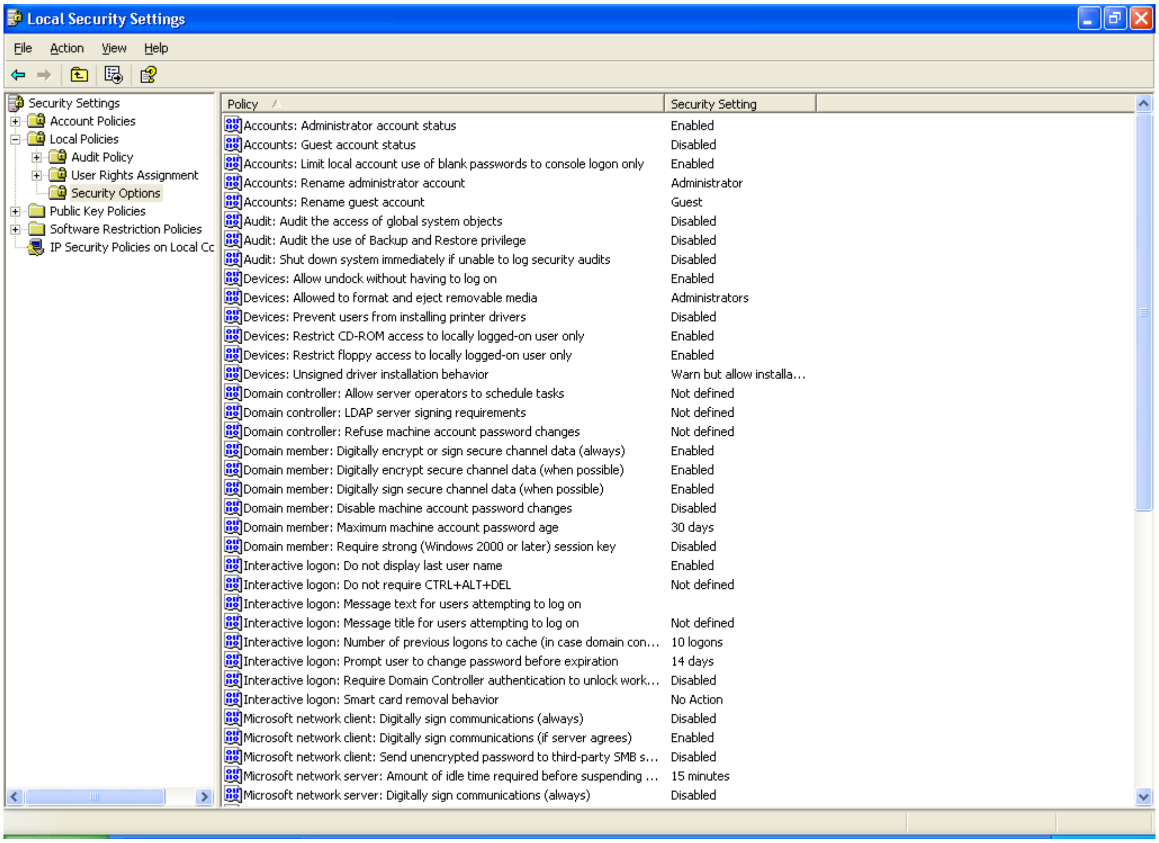
Computer:

From: First Event 1/17/2003 9:27:48 AM

To: Last Event 1/17/2003 9:27:48 AM

## ATTACHMENT 5

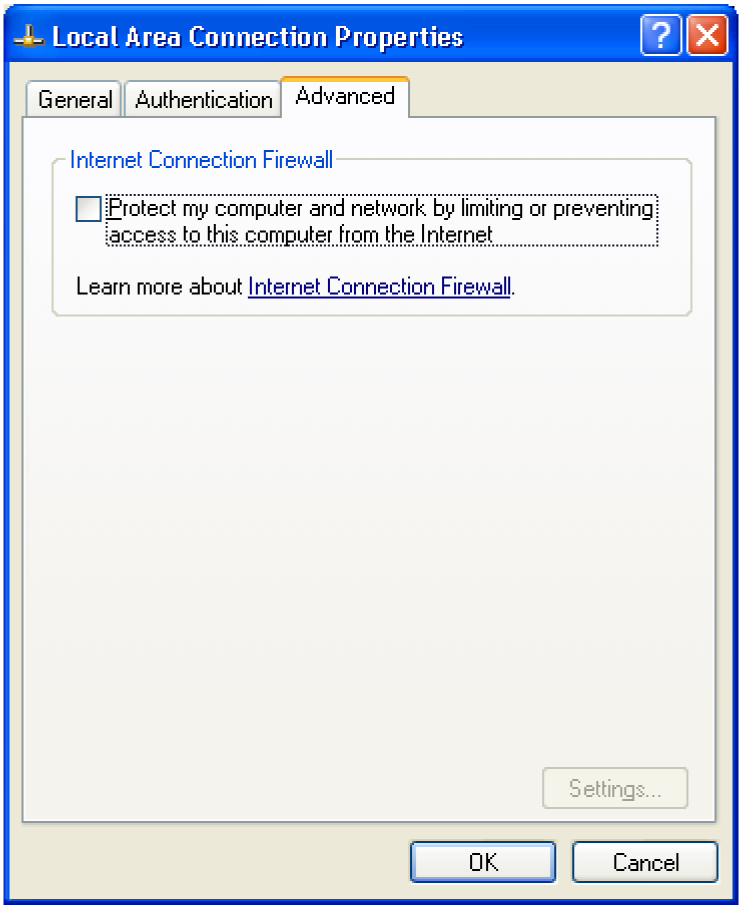
Microsoft Windows XP Professional Workstation Local Security Profile Properties:



| Policy | Security Setting |
|---|---|
| Accounts: Administrator account status | Enabled |
| Accounts: Guest account status | Disabled |
| Accounts: Limit local account use of blank passwords to console logon only | Enabled |
| Accounts: Rename administrator account | Administrator |
| Accounts: Rename guest account | Guest |
| Audit: Audit the access of global system objects | Disabled |
| Audit: Audit the use of Backup and Restore privilege | Disabled |
| Audit: Shut down system immediately if unable to log security audits | Disabled |
| Devices: Allow undock without having to log on | Enabled |
| Devices: Allowed to format and eject removable media | Administrators |
| Devices: Prevent users from installing printer drivers | Disabled |
| Devices: Restrict CD-ROM access to locally logged-on user only | Enabled |
| Devices: Restrict floppy access to locally logged-on user only | Enabled |
| Devices: Unsigned driver installation behavior | Warn but allow installa... |
| Domain controller: Allow server operators to schedule tasks | Not defined |
| Domain controller: LDAP server signing requirements | Not defined |
| Domain controller: Refuse machine account password changes | Not defined |
| Domain member: Digitally encrypt or sign secure channel data (always) | Enabled |
| Domain member: Digitally encrypt secure channel data (when possible) | Enabled |
| Domain member: Digitally sign secure channel data (when possible) | Enabled |
| Domain member: Disable machine account password changes | Disabled |
| Domain member: Maximum machine account password age | 30 days |
| Domain member: Require strong (Windows 2000 or later) session key | Disabled |
| Interactive logon: Do not display last user name | Enabled |
| Interactive logon: Do not require CTRL+ALT+DEL | Not defined |
| Interactive logon: Message text for users attempting to log on | |
| Interactive logon: Message title for users attempting to log on | Not defined |
| Interactive logon: Number of previous logons to cache (in case domain con... | 10 logons |
| Interactive logon: Prompt user to change password before expiration | 14 days |
| Interactive logon: Require Domain Controller authentication to unlock work... | Disabled |
| Interactive logon: Smart card removal behavior | No Action |
| Microsoft network client: Digitally sign communications (always) | Disabled |
| Microsoft network client: Digitally sign communications (if server agrees) | Enabled |
| Microsoft network client: Send unencrypted password to third-party SMB s... | Disabled |
| Microsoft network server: Amount of idle time required before suspending ... | 15 minutes |
| Microsoft network server: Digitally sign communications (always) | Disabled |

## ATTACHMENT 6

Microsoft Windows XP Professional Workstation Internet Connection Firewall Properties:

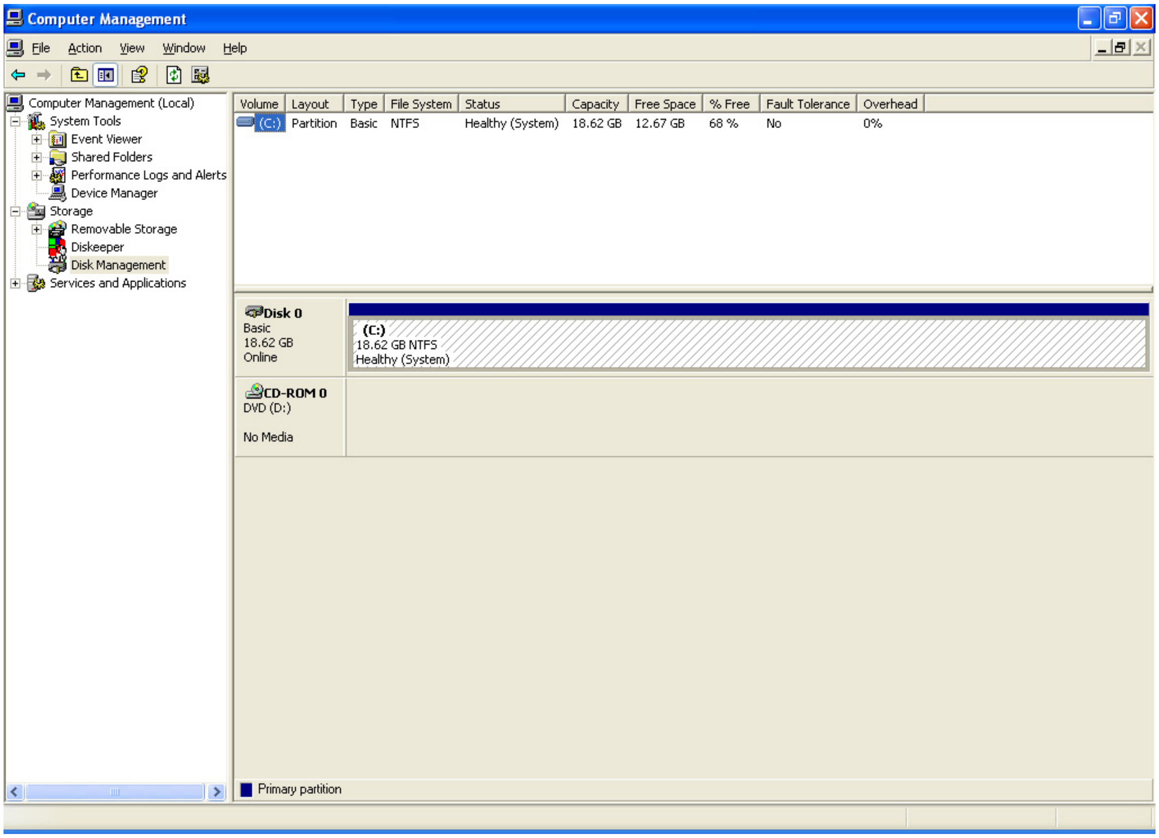

Local Area Connection Properties
General
Authentication
Advanced
Internet Connection Firewall
Settings...
OK
Cancel

□ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall.

## ATTACHMENT 7

Microsoft Windows XP Professional Workstation Hard Drive Partition Properties:



| Volume | Layout | Type | File System | Status | Capacity | Free Space | % Free | Fault Tolerance | Overhead |
|---|---|---|---|---|---|---|---|---|---|
| (C:) | Partition | Basic | NTFS | Healthy (System) | 18.62 GB | 12.67 GB | 68 % | No | 0% |

Disk 0
Basic
18.62 GB
Online

(C:)
18.62 GB NTFS
Healthy (System)

CD-ROM 0
DVD (D:)

No Media

■ Primary partition